Effective:
17 October 2025
Version 017

AUSTRALIAN PAYMENTS NETWORK LIMITED

ABN 12 055 136 519

A Company limited by Guarantee

Code Set

for

ISSUERS AND ACQUIRERS COMMUNITY FRAMEWORK

Volume 3
Acquirers Code

Commenced 1 July 2015

Australian Payments Network Limited
Telephone: (02) 9216 4888

Code Set for

ISSUERS AND ACQUIRERS COMMUNITY FRAMEWORK

Volume 3
Acquirers Code

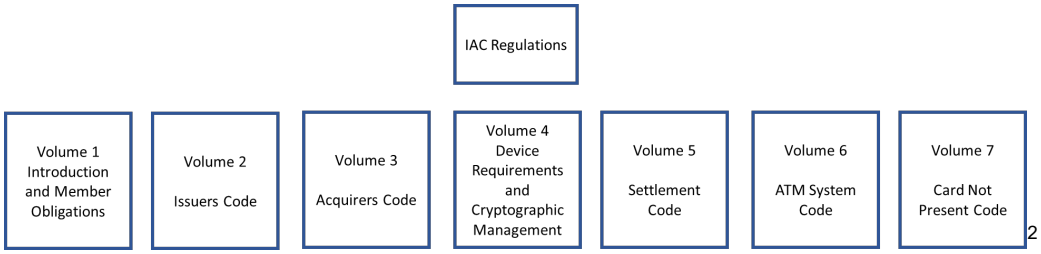
INDEX

PART 1 INTRODUCTION, INTERPRETATION AND DEFINITIONS

1.1 Purpose of this Code[1]

The IAC has been established to develop, implement and operate effective standards, policies and procedures to promote the efficiency, security and integrity of Australian Card Payments. These include minimum security standards, interoperability standards and value added services that support how payment cards are used throughout Australia.

These standards and requirements are contained within the IAC Code Set which is structured as follows:



[2]

This volume of the IAC Manual is intended for Acquirers and when used in conjunction with Volumes 1 and 4, contains requirements for PIN and Transaction security and management that are considered mandatory for all Acquirers participating within the IAC. Part 2 of this volume covers the high level requirements for PIN security, device functionality and interchange requirements; Part 3 covers the applicable device security requirements as well as the device management requirements applying to all Acquirers participating in the IAC. Part 4 of this volume, when read in conjunction with Volume 7, contains the requirements for Acquirers in dealing with Card Not Present Transactions, to mitigate the fraud associated with such Transactions.[3]

1.2 Interpretation[4]

Interpretations are located in a separate document entitled ‘Interpretation & Definitions'.

1.3 Definitions

Definitions are located in a separate document entitled ‘Interpretation & Definitions’.

Next page is Part 2

[1] Amended effective 1/1/19, version 008 r&p 002.18
[2] Amended effective 1/7/19, version 009 r&p 001.19
[3] Amended effective 1/7/19, version 009 r&p 001.19
[4] Amended effective 1/1/23, version 014 r&p 002.22

PART 2 TRANSACTION REQUIREMENTS[5]

(a) To ensure the security and integrity of the Australian payments environment, Acquirers must ensure that the following requirements are met at all times for all Card Payments.[6]

(b) The Acquirer is wholly responsible for ensuring that all Third Party Providers who are involved in processing Card Payments comply with the relevant provisions of this volume of the IAC Code.[7]

2.1 Functional requirements

2.1.1 *Account Selection*

At a minimum, device account selection should provide for cheque, savings and credit accounts.

2.1.2 *Record of Transaction*

(a) A Record of Transaction generated by a Terminal must be laid out in a clear manner, with all printed items shown in an unambiguous fashion. It must comply, at a minimum, with the standards detailed in the ePayments Code published by the Australian Securities and Investments Commission (ASIC).

(b) In addition to these requirements, any Card number included on the Record of Transaction must have at least four (4) digits excluded. The preferred method of truncation is to print the first six (6) digits and the last (3) digits of the Card number on the Record of Transaction.

(c) Card expiry dates should be excluded from Cardholder's Record of Transaction.

(d) For ATM Transactions, the Acquirer must be clearly identified on the Record of Transaction.

(Note: IAC Code Set Volume 6 (ATM System Code) contains additional requirements concerning a Record of Transaction for Transactions which involve an ATM Operator Fee).

[5] Last amended effective 1/1/19, version 008 r&p 002.18
[6] Last amended effective 1/1/19, version 008 r&p 002.18
[7] Last amended effective 1/1/19, version 008 r&p 002.18

2.2 PIN Security

Acquirers must ensure that:

(a) only Approved Devices are employed in Interchange;[8]

(b) the management of the Approved Devices meets the applicable management standards (see Part 3); [9]

(c) the key management practices employed comply with ISO 11568 or current AS 2805.6 series requirements; [10]

(d) PIN management procedures and practices comply with current ISO 9564-1requirements; [11]

(e) where a Transaction contains PIN data (bit 52), that PIN data must be formatted in accordance with one of the PIN block formats specified in ISO 9564.1 with the exception of formats 1and 2; and[12]

(f) All deployed ATM payment applications are either listed on the Approved Devices List prior to December 2021 or have been reviewed by the Acquirer or a trusted third party on behalf of the Acquirer and have been shown to contain no security vulnerabilities or other security weaknesses;[13]

as further detailed below.

2.3 Approvals[14]

2.3.1 *Approved Devices*[15]

(a) All Devices, Solutions and Non-Standard Technology involved in the production, distribution, selection, entering and transmission of plaintext Cardholder PINs, or cryptographic keys used to protect Cardholder PINs, Cardholder Data or Transactions, in the Interchange environment must meet the requirements set out in Part 3 and must be approved for use by the Company as specified in the IAC Code Set Volume 4 (Device Requirements and Cryptographic Management).[16]

(b) Only Approved Devices may be attached to the Interchange networks.

---

[8] Last amended effective 16/12/21, version 013 r&p 001.21
[9] Last amended effective 16/12/21, version 013 r&p 001.21
[10] Amended effective 17/10/25, version 017 r&p 001.25
[11] Amended effective 17/10/25, version 017 r&p 001.25
[12] Amended effective 21/11/16, version 004 r&p 002.16
[13] Amended effective 16/12/21, version 013 r&p 001.21
[14] Amended effective 1/1/19, version 008 r&p 002.18
[15] Amended effective 1/1/19, version 008 r&p 002.18
[16] Last amended effective 16/12/21, version 013 r&p 001.21

(c) Any Issuer or Acquirer, which proposes to:[17]

(i) implement any new Device, Solution or Non-Standard Technology (not currently covered by an existing Letter of Approval or other notification of approval described in the Device Approval Process); or

(ii) continue to employ an Approved Device which has reached or is about to reach its 'Letter of Approval' sunset date, unless the Company has renewed the device's Approval Period; or

(iii) implement any changes to an existing Approved Device's cryptographic devices, PIN or cryptographic key handling and management processing,

must apply for approval of the Device, Solution or Non-Standard Technology as required by clause 2.3.1(a) as if each is a new Device, Solution or Non-Standard Technology for the purposes of that clause.

2.3.2 *Software-based PIN entry on COTS (SPoC) Solutions [Deleted]*[18]

2.3.3 *Contactless Payments on COTS (CPoC) Solutions [Deleted]*[19]

2.3.4 *Non-Standard POI Technology [Deleted]*[20]

2.4 Cryptographic standards

2.4.1 *General*

(a) Acquirers must ensure that all cryptographic operations associated with the processing of Transactions satisfy current IAC cryptographic standards (see IAC Code Set Volume 4 (Device Requirements and Cryptographic Management). These include requirements regarding: [21]

(i) PIN encryption and Message Authentication across IAC Interchange Links;[22]

(ii) Message encryption across IAC Interchange Lines;[23]

(iii) PIN encryption and Message Authentication from Terminals and across Acquirer links; and

(iv) Key management practices.

[17] Amended effective 16/12/21, version 013 r&p 001.21
[18] Deleted effective 16/12/21, version 013 r&p 001.21
[19] Deleted effective 16/12/21, version 013 r&p 001.21
[20] Deleted effective 16/12/21, version 013 r&p 001.21
[21] Amended effective 1/1/19, version 008 r&p 002.18
[22] Amended effective 1/1/20, version 010 r&p 002.19
[23] Amended effective 1/1/20, version 010 r&p 002.19

2.4.2 *Message Authentication (for IAC Interchange Links)*[24]

(a) Message Authentication must apply to all IAC Interchange Links.

(b) The Message Authentication Code (MAC) must be calculated using DEA 3 or AES and an algorithm conforming to ISO 16609.[25]

(c) All interchange PIN and MAC cryptographic functions must be performed within an SCM that is an Approved Device.[26]

2.4.3 *Message Authentication (for Terminals)*

(a) Message Authentication must apply to all Terminal to Acquirer Links for all financial and key management messages.

(b) The MAC must be calculated using a block cipher listed in ISO 18033-3. Allowable block ciphers include DEA 3 with a 128 or 192 bit key and AES with 128, 192 and 256-bit keys.[27]

(c) The MAC algorithm must be:[28]

(i) listed in ISO/IEC 9797-1; or

(ii) part of an authenticated encryption algorithm specified in ISO/IEC 19772

2.4.4 *Privacy of Communication (for IAC Interchange Lines)* [29]

IAC Interchange Lines shall be subject to whole-of-message encryption, excluding communications headers, using DEA 3 or AES.[30]

2.4.5 *Privacy of Communication (for Terminals)*

(a) This clause applies to links between an EFTPOS Terminal and an Acquirer.

(b) For all Terminal to Acquirer links, Acquirers must ensure that privacy of communication complies with AS 2805.9 or any other privacy of communication standard approved by the Management Committee.

[24] Amended effective 1/1/20, version 010 r&p 002.19
[25] Amended effective 17/10/25, version 017 r&p 001.25
[26] Amended effective 16/12/21, version 013 r&p 001.21
[27] Last amended effective 17/10/25, version 017 r&p 001.25
[28] Inserted effective 1/1/25, version 016 r&p 001.24
[29] Amended effective 1/1/20, version 010 r&p 002.19
[30] Amended effective 17/10/25, version 017 r&p 001.25

(c) All application level data elements, including but not limited to fields P-45 (Track 1 data) and P-35 (Track 2 data), as defined in AS 2805.2, must be protected except those fields necessary to indicate the origin of the transaction and information required to correctly reconstruct the message. The latter may include the data required to derive the privacy key.[31]

(d) Where AS 2805.6.7 (DUKPT) is used to secure the dialogue between a Terminal and an Acquirer, compliance with AS 2805.9 must be achieved as per Appendix C of AS 2805.6.7.

2.4.6 *Key Management Practices – IAC Interchange Links*[32]

Key management practices for IAC Interchange Links must meet all applicable requirements of IAC Code Set Volume 4, clause 4.5.2.[33]

2.4.7 *Key Rolling Process for IAC Interchange Key Encrypting Keys (KEKs).*[34]

Key rolling process for IAC Interchange Key Encrypting Keys (KEK) must meet the applicable requirement of IAC Code Set Volume 4, clause 4.5.2(a).[35]

2.4.8 *Message Encryption for IAC Interchange Lines*[36]

Whole-of-message encryption must apply to IAC Interchange Lines and meet all applicable requirements of IAC Code Set Volume 4, clause 4.7.[37]

2.4.9 *IAC Interchange Line Cryptographic Management*[38]

IAC Interchange Line cryptographic management must meet all applicable requirements of IAC Code Set Volume 4, clause 4.7.1.[39]

2.4.10 *Key Management Practices for IAC Interchange Lines*[40]

Key management practices for IAC Interchange Lines must meet all applicable requirements of IAC Code Set Volume 4, clause 4.7.2.[41]

[31] Inserted effective 1/1/15, version 001 r&p 001.15
[32] Last amended effective 17/10/25, version 017 r&p 001.25
[33] Amended effective 17/10/25, version 017 r&p 001.25 to replace provisions with cross-reference.
[34] Last amended effective 17/10/25, version 017 r&p 001.25
[35] Amended effective 17/10/25, version 017 r&p 001.25 to replace provisions with cross-reference.
[36] Last amended effective 17/10/25, version 017 r&p 001.25
[37] Amended effective 17/10/25, version 017 r&p 001.25 to replace provisions with cross-reference.
[38] Last amended effective 17/10/25, version 017 r&p 001.25
[39] Amended effective 17/10/25, version 017 r&p 001.25 to replace provisions with cross-reference.
[40] Last amended effective 17/10/25, version 017 r&p 001.25
[41] Amended effective 17/10/25, version 017 r&p 001.25 to replace provisions with cross-reference.

2.5 Cardholder Data

All parties to Interchange, including Merchants, Acquirers, Third Party Providers and any intermediate network entities must maintain procedures and practices for preventing the unauthorised disclosure of Cardholder Data which, includes but is not necessarily limited to the: [42]

(a) Primary Account Number;

(b) Cardholder Name;

(c) Service Code;

(d) Expiration Date.

(As an example, compliance with the Payment Card Industry (PCI) Data Security Standard would be sufficient to meet this requirement.)

2.6 Sensitive Authentication Data

Sensitive authentication data, including but not limited to:

(a) Full magnetic stripe (or equivalent);

(b) CVC2/CVV2/CID;

(c) PIN/PIN Block;

must not be stored, outside of an SCD, subsequent to Authorisation.

2.7 Unauthorised Access Prevention

All parties to Interchange, including Acquirers, Issuers, Third Party Providers and any intermediate network entities must maintain procedures for avoiding any unauthorised access to or use of, the Interchange system through its own hardware, software, Interchange Lines and operational procedures which enable the exchange of authorisation and reconciliation of financial Transactions.[43]

Next page is Part 3

[42] Amended effective 1/1/19, version 008 r&p 002.18
[43] Amended effective 1/1/19, version 008 r&p 002.18

PART 3 DEVICE SECURITY

3.1 Terminal security

(a) A financial Terminal consists of a number of components, which may include some or all of the following: PIN Entry Device, printer, communications devices, customer/merchant interface, Acquirer application, IC Card reader and magnetic stripe reader. These components may be present in various configurations, dependent upon the function and capability of the Terminal.[44]

(b) Those components of a Terminal that provide cryptographic services and any services involved in requesting, reception and/or processing of the Cardholder PIN, the Cardholder Data or the Transaction must be approved for use by the Company (see IAC Code Set Volume 4 (Device Requirements and Cryptographic Management).[45]

3.2 EFTPOS Terminals[46]

3.2.1 *Physical Characteristics and Key Management Protocols*

If Terminals employ key-management schemes not specifically permitted in ISO 11568 or AS 2805.6 series, Acquirers may seek approval for their deployment from the Company. [47]

For the avoidance of doubt, a Terminal shall not rely on tamper evidence as its sole physical security characteristic (ISO 9564.1 clause 5.1). Terminals must also meet the following requirements:[48]

(a) when employing a “master/session key” key-management scheme (e.g., AS 2805.6.4); or[49]

(b) when employing a “unique key per Transaction” key-management scheme (e.g., AS 2805.6.7) they must meet, at a minimum, the requirements of a Physically Secure Device as defined in ISO 13491;[50]

(c) devices must generate and verify MACs as per ISO 16609 for all value Transaction messages; and[51]

(d) use one of the PIN block formats, excluding format 1, specified in ISO 9564.1. Format 4 is preferred. Format 8, here described, may also be used where required:[52]

---

[44] Amended effective 20/8/18, version 007 r&p 001.18
[45] Last amended effective 16/12/21, version 013 r&p 001.21
[46] Amended effective 20/8/18, version 007 r&p 001.18
[47] Last amended effective 17/10/25, version 017 r&p 001.25
[48] Last amended effective 20/8/18, version 007 r&p 001.18
[49] Amended effective 21/11/16, version 004 r&p 002.16
[50] Last amended effective 17/10/25, version 017 r&p 001.25
[51] Amended effective 17/10/25, version 017 r&p 001.25
[52] Last amended effective 17/10/25, version 017 r&p 001.25

(i) A format 8 PIN block may be used where a PIN Block is required but no PIN is available. The PIN block is constructed by the modulo 2 addition of two 64-bit fields formatted as follows:[53]

1. a plain text field[54]

Bit 1	5	9	13	17	21	25	29	33	37	41	45	49	53	57	61 64
C	N	R	R	R	R	R	R	R	R	R	R	R	R	F	F

and;

2. the account number field[55]

Bit 1	5	9	13	17	21	25	29	33	37	41	45	49	53	57	61	64
0	0	0	0	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	

Where:[56]

C	=	Control Field	• 1000 (binary)
N	=	PIN length	• 0000 (binary)
R	=	Random digit	• 4-bit binary field with each occurrence being randomly chosen form the range 0000 (zero) to 1111 (fifteen). • The resultant 48-bit random number shall be unique (except by chance) for each occurrence of a format 8 PIN block. • The random number shall not be transmitted in the clear.
F	=	Fill digit	• 1111 (binary)
0	=	Pad digit	• 0000 (binary)
A1 to A12	=	Account number	• Content is the 12 right-most digits of the primary account number (PAN) in 4-bit binary representation, excluding the check digit. • A12 is the digit immediately preceding the PAN's check digit. • If the PAN excluding the check digit is less than 12 digits, the digits are right justified and padded to the left with 0000 (zero). • Permissible values are 0000 (zero) to 1001 (nine)

and;

[53] Inserted effective 21/11/16, version 004 r&p 002.16
[54] Inserted effective 21/11/16, version 004 r&p 002.16
[55] Inserted effective 21/11/16, version 004 r&p 002.16
[56] Inserted effective 21/11/16, version 004 r&p 002.16

use only those hash algorithms specified in ISO TR-14742 Recommendations on Cryptographic Algorithms and their Use – Technical Report. Those algorithms must be implemented in accordance with the guidelines given in that technical report.

3.2.2 *PIN Entry Devices*

(a) PIN entry devices must be managed in accordance with the requirements of ISO 13491.[57]

(b) The Sponsor will submit to the Management Committee an annual compliance statement confirming compliance with Annexes A.3 and B.3 of ISO 13491.2 in respect of any PEDs employed in generating Interchange Transactions, Annexure B of IAC Code Set Volume 1 (Introduction and Member Obligations), provides the required confirmation.[58]

3.2.3 *Privacy Shielding*[59]

Where the device is designed and to be installed such that the device can be picked up and shielded from monitoring by the user's own body, or where the device, in itself, does not provide sufficient shielding and reliance is placed on the external physical environment, the Acquirer must ensure that the device is installed and managed in conformance with any vendor supplies rules and guidance as to how the visual observation is to be deterred.

3.2.4 *TCP/IP Terminal connectivity*[60]

The following requirements apply to all Terminals where TCP/IP protocols are used for communications.

(a) Terminal identification is mandatory and may be implemented in part (at the financial message protocol level) by using a (Terminal resident) MAC address as a (Terminal) serial number or the PIN Pad Identification Definition (PPID).

(b) Mutual authentication is mandatory and may be implemented at the network / transport layer (e.g., SSL, IPSec, et al) or at financial message layer (e.g., AS2805.6.5 series).

(c) Transport level message encipherment must be applied to the entire datagram encapsulating the financial message unless the Terminal is located on an Acquirer controlled private network.[61]

(d) End-to-end financial message encipherment must be provided using a method conformant to AS 2805.9.

---

[57] Amended effective 17/10/25, version 017 r&p 001.25
[58] Amended effective 17/10/25, version 017 r&p 001.25
[59] Amended effective 16/12/21, version 013 r&p 001.21
[60] Amended effective 1/1/19, version 008 r&p 002.18
[61] Amended effective 21/11/16, version 004 r&p 002.16

(e) All operating systems must be hardened.

(f) The Terminal must contain a firewall if it is based on a 'general purpose computer'.

(g) The Terminal must support a malware scanning application if it is based on a general purpose computer.

(h) No software on the Terminal will listen on any network service port, i.e., Terminal software may initiate "connect out" sessions only.

(i) The Terminal must support an active patch management process (to ensure that both the operating system and application environment is kept current and up to date to minimise exposure to any discovered flaws in those environments).

(j) The Terminal must, at a minimum, support DEA 3 encryption with full message encryption and authentication.[62]

(k) Only unique key per Transaction or dynamic session keys are permitted for Terminal key management. Terminals with dynamic session key changes (application level) are required to change session keys in accordance with IAC Code Set Volume 4, clause 4.8.2(a). Any remote support of merchant network and Terminals must be via a correctly configured and secured, remote access system.[63]

(l) The Terminal application software must be secured against unauthorised changes or substitution.

3.2.5 *Terminals Running Multiple Applications*[64]

The following requirements apply to all Approved Devices running multiple applications including non-payment applications.

(a) The Terminal shall meet the requirements of clause 3.2.4(e) to 3.2.4(i).

(b) The Terminal payment application software must be secured against unauthorised changes or substitution using cryptographic mechanisms.

(c) The Terminal shall authenticate all applications using cryptographic mechanisms.

(d) The Payment application and its associated data (especially PINs and cryptographic keys) must be protected from any interference or corruption caused by any other data or other application(s).[65]

[62] Amended effective 17/10/25, version 017 r&p 001.25
[63] Last amended effective 17/10/25, version 017 r&p 001.25
[64] Amended effective 1/7/15, version 001 r&p 001.15
[65] Inserted effective 16/12/21, version 013 r&p 001.21

(e) Payment and non-payment applications require individual evaluation and authorisation by the Acquirer, or a party explicitly trusted by the Acquirer, for each application to be deployed or updated. [66]

3.3 Security Control Modules

A Security Control Module (SCM) is a hardware device that provides an intentionally limited set of cryptographic services.

3.3.1 *Function set [Deleted]*[67]

3.3.2 *DEA-1*[68]

From 1 January 2013 all symmetric encryption functionality weaker[69] than DEA-3 must have been disabled within every deployed SCM.

3.3.3 *Security Control Module Management* [70]

(a) SCMs must be managed in accordance with the requirements of ISO 13491.2. The Sponsor must submit to the Management Committee an annual compliance statement confirming compliance with Annexes A.3, C.3, E.3 and either H.4 or H.5 in respect of any SCMs employed in the processing of Interchange Transactions. Annexure A of IAC Code Set Volume 1 (Introduction and Member Obligations) provides the required confirmation.[71]

(b) Where the SCM provides support for ISO format 1 PIN blocks, such functionality must be disabled in all Acquiring and switching systems.[72]

3.3.4 *Remote Management of Security Control Modules*

The requirements of this clause apply to systems which support remote access for the management of SCMs.

(a) SCM Access Requirements:

(i) SCMs must be located in a secure, protected network, separate from generic internal or external access;

(ii) there must be no uncontrolled connections between general internal and external networks;

(iii) SCMs must be accessible only to authorised hosts and authorised applications;

---

[66] Inserted effective 16/12/21, version 013 r&p 001.21
[67] Deleted effective 16/12/21, version 013 r&p 001.21
[68] Amended effective 17/10/25, version 017 r&p 001.25
[69] See ISO TR14742 for an understanding of which algorithms are weaker than DEA-3
[70] Amended effective 20/8/18, version 007 r&p 001.18
[71] Amended effective 17/10/25, version 017 r&p 001.25
[72] Amended effective 16/12/21, version 013 r&p 001.21

(iv) for TCP/IP implementations:

(A) the SCM environment must be protected at a minimum by an IPS or IDS between the perimeter network firewall and the remote management device;

(B) stateful firewalls must protect all external entry points to the SCM environment; and

(C) such firewalls must log and monitor all inbound and outbound traffic to the SCMs;

(v) there must be a procedure, which is audited on a regular basis, for the rapid disablement of known/suspected compromised remote management devices.

(b) Management of SCM Remote Management Solutions:

(i) Remote Management Solutions may only be used with AusPayNet approved SCMs.

(ii) All SCM Remote Management Solutions must have been approved as part of the Device Approval Process.[73]

(iii) Remote management devices may only be deployed in a minimally controlled environment, a controlled environment or a secure environment as per Annex H of ISO 13491.2. At a minimum:[74]

(A) the storage of the Remote Management Solution must be under dual control;

(B) the operation of the Remote Management Solution must be under dual control; and

(C) while the Remote Management Solution is in operation access must be restricted to authorised personnel.

3.4 Key Loading and Transfer Devices

(a) Devices used in the initial cryptographic key loading of PEDs must be managed in accordance with the requirements of ISO 13491.2.[75]

[73] Amended effective 16/12/21, version 013 r&p 001.21
[74] Amended effective 17/10/25, version 017 r&p 001.25
[75] Amended effective 17/10/25, version 017 r&p 001.25

(b) The Sponsor must submit to the Management Committee an annual compliance statement confirming compliance with Annexes A.3, E.3 and F.3 of ISO 13491.2in respect of any devices employed in the initial loading and transfer of PED cryptographic keys Annexure B of IAC Code Set Volume 1 (Introduction and Member Obligations), provides the required confirmation.[76]

3.5 TCP/IP Host Requirements [77]

The following requirements apply to host systems which support Terminals using the TCP/IP protocol for communications:

(a) stateful firewalls must protect all external entry points to the host environment;

(b) strong financial message protocol validation must be performed between Terminals and acquiring hosts;

(c) acquiring host must be located in a secure, protected network separate from generic internal or external access;

(d) production Security Control Modules must be accessible only to authorised production hosts and authorised production applications. Where connected via TCP/IP they must be on a separate, stand-alone network;

(e) there must be no uncontrolled connections between general internal and external networks and Terminal/SCM networks (assuming they are all TCP/IP);

(f) the host environment must provide, at a minimum, an IPS or IDS between the perimeter network firewall and acquiring host;

(g) the host system must support appropriate threat management techniques relevant to the host's operating platform, such as malware protection with up to date signatures and maintenance, vulnerability patching, etc.;

(h) the host must provide a mechanism for the rapid disablement of known/suspected compromised Terminals.

3.6 Key Injection Facility Assessment

3.6.1 *Request Assessment*

An Acquirer may request the Company conduct an assessment of a Key Injection Facility for the purposes of verifying compliance with certification requirements under IAC Code Set Volume 1 (Introduction and Member Obligations). This clause broadly outlines the process for assessment of a Key Injection Facility by the Company on an Acquirer's behalf.

[76] Amended effective 17/10/25, version 017 r&p 001.25
[77] Amended effective 1/1/19, version 008 r&p 002.18

In this clause, "Applicant" means the Acquirer on whose behalf the Company agrees to conduct an assessment of a Key Injection Facility.

3.6.2 *Nomination for Assessment*

An Applicant should initiate the assessment process by submitting to the Company:

(a) a written request that the Company assess a nominated Key Injection Facility on its behalf;

(b) evidence of the consent of the Key Injection Facility to the conduct of the assessment by the Company in accordance with this clause 3.6.2, such consent to be evidenced by a Key Injection Facility Assessment Agreement executed by the Key Injection Facility; and

(c) all relevant additional information, including technical materials and evidentiary matters relevant to the Applicant's certification requirements with respect to key injection practice.

3.6.3 *Assessment Process*

(a) The Company will assess the performance of the Key Injection Facility in relation to the Company's standards and the Applicant's requirements. The Key Injection Facility must comply with the standards and requirements set out in Annexure B, together with such additional requirements as may be applicable to the Applicant's circumstances or requirements.

(b) The Key Injection Facility assessment process comprises such business reviews, technical reviews and on-site visits as may be necessary to enable the Company to properly assess the compliance of the Key Injection Facility with applicable requirements.

(c) Once a Key Injection Facility has been assessed by the Company as compliant with the applicable requirements, the Acquirer may rely on the assessment only for the purposes of certification under IAC Code Set Volume 1 (Introduction and Member Obligations). The Company may require, at its sole discretion, a Key Injection Facility to provide evidence of its continued compliance with assessment requirements triennially. The Company in its sole discretion may determine whether any other person, including any other Acquirer, may rely on the assessment for certification purposes.

Next page is Part 4

PART 4 CARD NOT PRESENT TRANSACTIONS[78]

4.1 Compliance Provisions

Each Acquirer must comply with the obligations in Part 3 clause 3.2 of the IAC Code Set Volume 7 (Card Not Present Code).

The next page is Annexure A

[78] Amended effective 1/1/20, version 010 r&p 002.19

Annexure A. KEY INJECTION FACILITY REQUIREMENTS

[Informative]

This Annexure will be used by the company in carrying out an assessment of a Key Injection Facility as set out in clause 3.6 of this Code. It provides the assumptions, scope references and definitions in support of the Key Injection Facility Requirements provided in Annexure B.

A.1 Assumptions

(a) As only AusPayNet approved SCDs are used for key handling, i.e., HSMs, KLDs and Terminals, it is assumed that these devices will only perform in their accredited manner. Therefore, no requirements have been included here that would have been checked during the SCD approval process (i.e., key lengths, algorithms, randomness and uniqueness of keys). This also applies to the tamper responsiveness of the PEDs after key injection.[79]

(b) KLDs have their own set of requirements which will not need to be rechecked by the facility. This includes how the device is handled once it has been securely dispatched from the facility, i.e., requirements on how keys are transferred from the KLD into a Terminal.[80]

A.2 Scope

(a) The Key Injection Facility is considered to be the entire facility that is responsible for generation of the keys for injection into a PED through to loading of these keys into the PED.

(b) Annexure B, sets out the minimum requirements for protecting these keys; however it is understood that the environment in which the KIF operates may provide suitable mitigation in the event the requirements are not fully achieved.

(c) The scope of this part is limited to those requirements (both physical and operational) necessary for a KIF to meet. It covers:

(i) the generation of the initial cleartext keys or key components to be loaded into a Terminal or a KLD (used to transfer keys from the KIF to a Terminal);[81]

(ii) the secure loading of cleartext keys or components into Terminals or KLDs within the KIF;[82]

(iii) the secure management of any key generation device, Terminals or KLD during the time it is under the control of the KIF;[83]

[79] Amended effective 20/8/18, version 007 r&p 001.18
[80] Amended effective 20/8/18, version 007 r&p 001.18
[81] Amended effective 20/8/18, version 007 r&p 001.18
[82] Amended effective 20/8/18, version 007 r&p 001.18
[83] Amended effective 20/8/18, version 007 r&p 001.18

(iv) the loading of a keys, as part of the manufacturing process, which are subsequently used by the KIF;

(v) key management between KIF and manufacturer, if required;

(vi) key management between the KIF and acquirer, if required; and the secure receipt and dispatch of PEDs or KLDs to and from the KIF; and

(vii) CAs and RAs which operate under a PKI scheme and may be used as part of a remote key initialisation scheme.

(d) The types of keys subject to the requirements outlined in this part are application-level keys used by, or injected by, the KIF into a Terminal as part of injection and initialisation process associated with the device. Such key types include:[84]

(i) Asymmetric initialisation master keys, such as manufacturer, sponsor, and TCU public & private keys;

(ii) Symmetric initialisation master keys, such as manufacturer, sponsor, and TCU master and derived keys;

(iii) the initial keys that the KIF is responsible for are any keys generated by the KIF, or received and managed by the KIF, which lead up to the establishment in the Terminal of the initial key common to the acquirer and Terminal.[85]

(e) This part does not cover:

(i) the manufacturing process of Terminals, including any loading of firmware etc. by the manufacturer, except where the manufacturer generates and loads a key as part of the manufacturing process. In the latter case, the manufacturer's key injection facility must comply with these requirements;[86]

(ii) any subsequent storage or dispatch of the device by the manufacturer to the KIF;

(iii) the manual loading of the initial keys into remote Terminals by a KLD;[87]

(iv) network or transport-layer keys, such as those used to provide full stream encipherment of traffic independent from the devices payment application (e.g., SSL/TLS, IPSec, etc.,), nor does it address any application signing keys used to secure the payment application on the device.

[84] Amended effective 20/8/18, version 007 r&p 001.18
[85] Amended effective 20/8/18, version 007 r&p 001.18
[86] Amended effective 20/8/18, version 007 r&p 001.18
[87] Amended effective 20/8/18, version 007 r&p 001.18

(f) There are three phases for a device from manufacture through to installation for its intended use. The first is the manufacturing process itself. The first phase is not covered by these requirements. The second is the phase is post-manufacturing, from the time that the manufacturing process has been completed until the installation of the first key into the device. The third phase is pre-use, the period from the time the device is loaded with its initial key until it is installed for use. These requirements only cover the device from the post-manufacturing phase through to the pre-use phase when it is dispatched from the KIF plus any device returned from the field for reinjection.

(g) The intention of these requirements is to ensure that no Terminal goes into operation with compromised keys which could lead to a loss of customers' PINs. Although facilities whose processes and systems meet these requirements may not be able to prevent the compromise of keys used in the facility, any such compromise should be detected with a high degree of certainty before the compromised keys can be used. This can be achieved by utilizing appropriate factors of:[88]

(i) device characteristics;

(ii) device management; and

(iii) environment.

A.3 Key Injection Facility Audit Guide

The Key Injection Facility Audit Guide, v3.01F1F[89] should be used in conjunction with this document and provides additional information on how certain of the requirements are to be met.

A.4 References

(a) The following documents were used in the development of these requirements:

(i) AS 2805.6.1;

(ii) ANSI X9.24 2004;

(iii) ISO 11568-2;

(iv) ISO 13491-2 2005;

(v) CECS Manual – 2008;

(vi) Visa PCI-PIN Security Requirements (Annex B) – Jan 2008;

[88] Amended effective 20/8/18, version 007 r&p 001.18
[89] Available on the AusPayNet Extranet at https://extranet.auspaynet.com.au/extranet/cs0corpdocs.nsf/NDX/KIF_AUDITGUIDE_CURRENT?OpenDocument&Login

(vii) ANSI X9 TG-3 – 2006;

(viii) AS 2805.14.1;

(ix) Visa Cryptographic Key Injection Facility: Auditor's Guide v1.0, Jan 2008;

(x) ISO 11568-4;

(xi) ISO 11770-3;

(xii) MasterCard PCI-PIN Security Requirements – March 2008.

(b) Appendix A of the KIF Audit Guide provides a cross reference table indicating how the requirements in the reference documents are covered by the requirements in this document. The original documents can be used to clarify the intention behind the requirements however, where a discrepancy might exist, this part will take precedence.

A.5 Definitions

For the purposes of this part, the following definitions apply.

"**Approved Device**" [Deleted][90]

"**Asymmetric Key Pair**" means the two related keys, called the public key and the private key that are used with the DEA 2 asymmetric algorithm.

Note: DEA 2 is specified in AS 2805.5.3.

"**Certification Authority**" and "**CA**" means an entity which issues digital certificates for use by other parties. It is an example of a trusted third party. CAs are characteristic of many public key infrastructure (PKI) schemes.

"**Cipher Text**" means plain text that has been enciphered.

"**Cleartext Key**" has the same meaning as Plaintext Key.

"**Digital Certificate**" means a digital certificate is used to bind together a public key with an identity in the form of a public key certificate. It contains information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual.

"**Dual Control**" means the process of utilizing two or more entities (usually persons) operating in concert to protect sensitive functions or information whereby no single entity is able to access or use the materials.

"**Key Injection Device**" and "**KID**" means an approved SCD which is loaded with keys for injection into devices within the KIF, e.g., is used to inject acquirer supplied keys into a PED.

[90] Deleted effective 16/12/21, version 013 r&p 001.21

"**Key Injection Facility**" and "**KIF**" means a secure facility which contains an SCD for key generation and/or injection. The level of security will be determined by the security requirements of the SCD(s) used within the facility.

"**Key Pair**" has the same meaning as Asymmetric Key Pair.

"**Local Registration Authority**" and "**LRA**" means an optional part of a PKI that maintains users' identities from which CAs can issue digital certificates.

"**Plaintext Key**" means an unenciphered cryptographic key or key component, which is used in its current form.

"**Private Key**" means that key of an entity's asymmetric key pair, which can only be used by that entity. In the case of an asymmetric signature system, the private key defines the signature transformation.

> *Note: The term private key differentiates this key from the secret key of a symmetric algorithm.*

"**Public Key**" means that key of an entity's asymmetric key pair which can be made public. In the case of an asymmetric signature system the public key defines the verification transformation.

"**Registration Authority**" has the same meaning as Local Registration Authority.

"**RSA**" means the name given to an algorithm for public-key cryptography.

"**Secret Key**" means a cryptographic key used with a symmetric cryptographic algorithm that is uniquely associated with one or more entities and must not be made public.

"**Split Knowledge**" means a condition under which two or more parties, separately and confidentially, have custody of components of a single key that, individually, convey no knowledge of the resultant key.

"**Symmetric Key**" means a secret key used with a symmetric cryptographic algorithm which uses the same key for encipherment and decipherment.

"**Tamper Evidence**" means a process that makes unauthorised modification to the device easily detected.

"**Tamper Responsiveness**" means a process that detects the intrusion attempt and destroys the sensitive contents of the device.

Next page is Annexure B

Annexure B. KEY INJECTION REQUIREMENTS

[Informative]

This Annexure, to be used in conjunction with Annexure A, contains the Key Injection Facility Requirements to be used by the Company in carrying out an assessment of a Key Injection Facility as set out in clause 3.6 of this Code.

B.1 Key Injection Facility (KIF)

This facility is a secure environment which encloses the key injection process, housing the key generation/injection device plus any Terminals, PEDs and KLDs whilst they are being loaded and prior to securing for dispatch. The level of security afforded by this facility will depend on the minimum security requirements of the devices housed and used within that facility.[91]

KIF Requirements		Ref[92]
B.1.1	Key Injection Facilities shall inject keys only into approved SCDs. This includes, but is not limited to, Terminals, PEDs and KLDs. The SCDs shall be approved by AusPayNet for their intended purpose.[93]	5
B.1.2	Key Injection Facilities that include hardware devices/systems for managing keys (e.g., generation and storing) shall ensure those hardware devices/systems are approved by AusPayNet or PCI as per these requirements or comply with the requirements of clause B.2.18. This includes HSMs and any associated system, such as a PC, to which the HSM is attached and that the cleartext keys or components pass through.	5
B.1.3	A KIF, including all processes related to key management (e.g., key generation and injection), shall be implemented securely within an environment which meets the definitions of a Controlled or a Secure environment in Annex H of Reference 4 (see KIF Audit Guide), and shall be operated under dual control.	3
B.1.4	The environment shall remain secure until all keys or other secret data and useful residue from such secret data and have been removed from the environment or destroyed.	2

[91] Amended effective 20/8/18, version 007 r&p 001.18
[92] This reference number refers to numbers in the "Key Injection Requirements Cross Reference Table" document in the KIF Audit Guide (refer to clause A.3).
[93] Amended effective 20/8/18, version 007 r&p 001.18

KIF Requirements	Ref[92]
B.1.5 Any hardware used in the key injection process shall be monitored and a log of all key-loading activities maintained for audit purposes. This log must be protected from unauthorised modification.	34
B.1.6 Auditable records shall be maintained on all SCDs processed by the facility, from the time of receipt through to dispatch to ensure detection of lost or stolen equipment. The record (which must be protected from unauthorised modification) should contain but is not limited to the following information: (a) sender; (b) receipt note number; (c) manufacturer; (d) serial number of the device; (e) operations carried out on device. (f) recipient; (g) confirmation of receipt; and (h) dispatch note number.	
B.1.7 All SCDs received by the facility shall be accounted for and any discrepancy between the quantity and serial numbers of the devices sent and of those received shall be notified to the sender and owner and investigated.	
B.1.8 All SCDs dispatched from the facility shall be accompanied by an itemized record of the devices dispatched. The recipient shall notify the KIF of any discrepancy between the record of items sent by the facility and the SCDs actually received.	
B.1.9 The KIF operator shall ensure that any new staff involved within the KIF or who have access to keys or key components, are subject to appropriate probity checking (e.g., identity verification, reference check, criminal record check) such as those required for Australian Financial Services License holders for employment of Responsible Officers (RO) as outlined in ASIC policy statement (PS 146) or equivalent.	

KIF Requirements		Ref[92]
B.1.10	Documented procedures exist and are demonstrably in use for all processes related to the operation of the KIF, including key injection, and all involved staff shall be trained and competent in the use of these procedures.	33,82 & 88
B.1.11	No wireless network connectivity is allowed to or from the KIF.	
B.1.12	Where the KIF participates in remote key establishment and distribution applications the following additional requirements of References 6 and 12, where they relate specifically to remote key establishment and distribution applications: (a) Question 19 - Single Purpose Keys; (b) Question 22 - Key Compromise Procedures; (c) Question 25 - Limit Key Access; (d) Question 28 - Key Administration Procedures; and (e) Question 31 - SCD Procedures; shall be used.	

B.2 Key Generation (KGD) / Key Injection Devices (KID)

(a) These devices are used to generate and inject keys into a Terminal, PED or KLD. They may generate those keys or inject preloaded keys from an acquirer. To enable the loading into the device "preloaded keys" and/or sending generated keys, they will need the functionality to enable the loading of keys such as transport keys or other acquirer related keys. The handling of the acquirer related keys will be managed in accordance with the General Key Management requirements stated in clause B.5 below.[94]

(b) The key generation device may be a purpose built SCD or it may be a device which contains an SCD for the key generation and storage. Accordingly, it should not be assumed that in the following requirements the term device means only an SCD unless expressly described as such. All attached cables to the device (other than the power cable) must be treated as an integral part of the device.

[94] Amended effective 20/8/18, version 007 r&p 001.18

(c) A KID is either loaded with keys for injection into a Terminal or PED or it may contain a KGD to generate the keys for injection. The KID will use an SCD to manage the storage and generation of keys. These devices (KIDs) are not used to transport keys to Terminals or PEDs outside the KIF.[95]

(d) A KID is loaded with keys for injection into a Terminal or PED, e.g., the keys are generated by a acquirer and loaded into the KID. The KID will use an SCD to manage the storage and injection of keys. These devices (KIDs) are not used to transport keys to Terminals or PEDs outside the KIF.[96]

(e) There are two types of device that can be used to generate and inject keys. One type of device requires tamper responsiveness and tamper evidence because a compromise of the device could disclose keys previously generated or injected by the device prior to the compromise. The other type of device requires only tamper evidence because the device retains no information that, if disclosed, could disclose any key that had been injected into a cryptographic device prior to the compromise.

KIF Requirements	**Ref**
B.2.1 The generation, and/or storage of plain text keys shall be carried out within an AusPayNet approved SCD, e.g., HSM. The approval process shall include evaluation/approval of any functions specifically required for this function. Where the KGD comprises a personal computer and an SCD: (a) the SCD is to be integral to the device or directly connected (e.g., serially); (b) all openings on the device that are not used for key injection are securely sealed in a tamper-evident and auditable manner. Examples include USB ports, unused serial connections, PCMCIA slots, etc.	5, 11

[95] Amended effective 20/8/18, version 007 r&p 001.18
[96] Amended effective 20/8/18, version 007 r&p 001.18

KIF Requirements	Ref
B.2.2 Where the device (KID) handles clear text secret or private keys, at a minimum, the following controls shall be enforced for the device to be classified as an approved KID classified as an approved KID: (a) All key generation and/or storage is handled in accordance with Requirement B.2.1 by using an SCD which is an Approved Device (KGD); (b) That device (KID) shall meet the requirements of Annex F of Reference 4 (see KIF Audit Guide) and be approved for this use by AusPayNet.	
B.2.3 Where an approved KGDs and KIDs are used then: (a) Where there is a network connection then: (i) Any connection made from or to those devices is mutually authenticated; (ii) that device shall not send or receive cleartext keys or components via the network connection; (iii) the devices must be on a dedicated network segment which is isolated from other network devices; (iv) all communications into and out of those devices is enciphered; (v) the network connection between the two devices is required to be firewalled at both network endpoints and is required to provide an additional security layer over any application later cryptographic protection (e.g., IPsec); (vi) only ports required for the KIF functionality are open; and (vii) the network connection shall not be able to be used to compromise or manipulate any process carried out by those devices; (b) The device used for the key injection function, plus any cables, keypads or other attachments, are maintained under dual control at all times; (c) That device maintains an auditable log of all operations which includes as a minimum, the following information: (i) The time and date of any operation, including power on and off;	

KIF Requirements	Ref
(ii) Details of the operation being performed; (iii) The PPID and serial numbers of any device injected with keys; (iv) User sign-on at system and operator levels; (d) The logs shall be cryptographically authenticated such that an altered or missing log activity can be detected; (e) Hardware use is monitored and logs of key loading activity are maintained; (f) That device is started from a powered off position for each key loading activity; (g) The personnel responsible for the systems administration of the device shall not have authorized access into the room – they shall be escorted by authorized key injection personnel, and they shall not have user IDs or passwords to operate the key injection application; (h) The key injection personnel shall not have system's administration capability on the device; (i) The device shall not be able to boot from external media (such as floppies or CDs). It shall boot from the hard drive only where applicable; (j) Manufacturer's default passwords shall be changed.	
B.2.4 Where an approved Key Injection device (KID) is not used, the following minimum controls shall be enforced: (a) The device shall be standalone; (b) The KID shall comply with clause B.2.1 (c) The device, or any of its components, shall not be removed from the KIF before destroying al memory components; (d) Shall adhere to clause B.2.3(b) to B.2.3(j), above where applicable. Please note, AusPayNet intends to enforce the use of approved KIDs at some future date to be determined by the IAC committee of management.	

KIF Requirements	Ref
B.2.5 No person with existing or prior access to any mechanism used to enforce dual control on the KGD/KID (e.g., password or physical key) has existing, prior, or future access to any other mechanism used to enforce dual control on that device.	
B.2.6 Plaintext keys shall never be written to any form of non-volatile storage outside of the tamper responsive envelope of an approved SCD, e.g., PED.	
B.2.7 Keys shall not be installed in any KGD/KID until it has been inspected by qualified staff, i.e., staff who have been specifically trained for this role, and a reasonable degree of assurance has been reached that the KGD/KID is an authentic device and has not been subject to any unauthorised physical or logical modifications or substitution. This assurance may take the form of, but not limited to, one or more of the following methods using appropriate guidelines from the supplier on how this is to be done: (a) Physical inspection and/or testing of the equipment immediately prior to key loading; and (b) Physical protection of the equipment. (e.g., bonded carrier, device authentication code injected by Terminal vendor and verified on receipt, tamper evident packaging, etc.). (c) The device is delivered with secret information to allow the KIF to ascertain that the device is genuine and not compromised providing the secret information has not been erased.	37
B.2.8 The key generation device will not output any plaintext key except under dual control. Such dual control shall be enforced by the KGD/KID or the PED requiring that at least two passwords be correctly entered within a period of no more than five minutes, before the device will output/accept a key. The device shall ensure that passwords are at least 5 characters long and the characters shall be a mixture of alphanumeric where available.	12
B.2.9 Where an asymmetric key pair is generated for transfer into another device by a KGD/KID that will not use the key pair, then the private key of the key pair and all related secret seed elements shall be 'zeroised' or otherwise permanently deleted immediately after the transfer to the target device has been ensured.	14

KIF Requirements		Ref
B.2.10	The transfer mechanisms by which plaintext keys, key components or passwords are transferred into or out of the KGD/KID are protected and/or inspected so as to prevent any type of monitoring that could result in the unauthorized disclosure of any keys, key components or passwords. This shall take into account all aspects of monitoring, including the use of surveillance cameras. This will require all cables and attachments to be managed under dual control.	30
B.2.11	All plain text keys that have been injected into a device are to be maintained in one of the acceptable key forms as stated in this document. These keys shall not be retained by the KIF after the keys have been injected and are in the possession of the sponsor of the device.	28
B.2.12	Controls are in place to ensure that no information remains within any KGD/KID that is to be removed from the KIF which could disclose any cryptographic key that ever existed within that device.	29
B.2.13	Controls are in place to detect the unauthorized reinstallation of a KGD/KID previously removed from a facility.	31
B.2.14	Controls are in place to detect the unauthorized removal of the KGD/KID from, and its unauthorized replacement back into, its authorized location.	32
B.2.15	All keys that have been used, or potentially could be used, in a KGD/KID that has been removed from service shall be destroyed. If this cannot be accomplished then the device shall be physically destroyed so that no keys can be disclosed nor the device placed back in service again. This requirement does not include keys that have been already deployed in the field.	86

KIF Requirements	Ref
B.2.16 Controls are in place to detect the unauthorized removal of the KGD/KID from, and its unauthorized replacement back into, its authorized location. This could take the form of: (a) mechanisms such that the removal of that device from its operational location will cause the automatic erasure of the cryptographic keys contained within that device; (b) the KGD/KID is stored, under dual control, in a safe or room that cannot feasibly be penetrated, and each incident of opening or closing the safe or room is recorded under dual control.	16
B.2.17 Unauthorized use of the KGD/KID, when in active use, is prevented or detected by means such as the following: (a) the KGD/KID has functional or physical characteristics (e.g., passwords or physical high-security keys) that prevent use of that device except under dual control, and when in that useable state, that device is under the continuous supervision of at least two trusted people who are qualified to detect and able to observe any attempted unauthorized access, and able also to prevent such access before it is successful; (b) the KGD/KID is at all times either locked or sealed in a tamper-evident cabinet or else is under the continuous supervision of at least two authorized people who ensure that any unauthorized use of that device would be detected.	17 & 19
B.2.18 When the KGD/KID is not in active use, any unauthorized access to that device is prevented by means such as the following: (a) the facility (e.g., room) where the KGD/KID operates has sufficient supervision and controls to prevent any unauthorized access to that device that would allow alteration to that device or disclosure of any key or other sensitive data without detection; (b) the KGD/KID is stored, under dual control, in a safe that cannot feasibly be penetrated without detection, and each incident of opening or closing the safe is recorded under dual control.	18 & 20

KIF Requirements	Ref
B.2.19 Any physical keys used to secure, unlock or operate a KGD/KID are carefully controlled, and available only to authorized persons.	22
B.2.20 The KID is used to inject a plaintext key into a cryptographic device only under the direct supervision of at least two authorized people, both of whom ensure that there is no "bug" or other disclosing mechanism on the path that the key traverses from the KID to the target device.	50

B.3 Procedures for Handling Target Devices

The target devices referred to in this Part are either PEDs or Terminals. Requirements for Key Loading Devices (KLDs) which do not have key generation or PIN handling functionality are covered in clause B.4. It is important to ensure that no unauthorised access to the device remains undetected from the time of manufacture through to it being put into use.[97]

Prior to an initial key being loaded, the target devices require only tamper evidence because the device retains no information that, if revealed, could disclose any key that had been injected into the device prior to the compromise. Terminals or PEDs that have a public key (or key pair) installed as part of the manufacturing process shall be in a tamper responsive state once the public key (or key pair) has been installed. These keys may be for authenticating subsequent application loads and/or key loads.[98]

[97] Amended effective 20/8/18, version 007 r&p 001.18
[98] Amended effective 20/8/18, version 007 r&p 001.18

KIF Requirements	Ref
B.3.1 Keys shall not be installed in any SCD until it has been visually inspected by staff, who are trained to detect a non-authentic or tampered device, and a reasonable degree of assurance has been reached that the SCD is an authentic device and has not been subject to any unauthorised physical or logical modifications, or substitution. This assurance may take the form of, but not limited to, one or more of the following methods using appropriate guidelines provided by the supplier on how this is to be done: (a) Physical inspection and/or testing of the equipment immediately prior to key loading; and (b) Physical protection of the equipment (e.g., bonded carrier, device authentication code injected by Terminal vendor and verified on receipt, tamper evident packaging, etc.); (c) The device is delivered with secret information to allow the KIF to ascertain that the device is genuine and not compromised providing the secret information has not been erased.	37
B.3.2 Any device, once it has been injected with keys, is controlled so as to prevent or detect unauthorized access to it, with records kept and audited so as to detect and report unauthorised substitution, theft or loss.	39
B.3.3 Controls are in place to ensure the destruction of any existing keys in a device returned to the KIF prior to the injection of new keys into that device.	
B.3.4 The distribution and loading of keys into a PED shall be performed under dual control using one of the following techniques: (a) manual, e.g., key component entry via a key pad when device is in a sensitive state; or (b) electronic direct loading, e.g., direct key injection via a cable from the originating device.	41 & 43
B.3.5 The action of loading a key puts the device in a mode that activates all tamper protection mechanisms within the device unless it is in that mode.	42

KIF Requirements	Ref
B.3.6 KIFs shall ensure that unique symmetric and/or private keys are loaded into each device. The same key(s) shall not be loaded into multiple devices. Public keys (certificates) may be common to a group of devices.	8
B.3.7 Where keys are derived for injection into various types of devices, the same key should not be derived for multiple devices, except by chance.	8
B.3.8 Controls are in place to detect the unauthorized replacement of a Terminal or PED previously removed from a facility.[99]	31
B.3.9 Upon inspection of a device, where there is any evidence of tampering or doubt about tampering, the acquirer shall be notified immediately.	

B.4 Key Loading (KLD) / Key Transport Devices (KTD)

A KLD is an SCD used to load plain text keys into an SCD outside of the KIF, i.e., load keys into a PED in the field. A KTD is an SCD used to transfer keys between an SCD in the KIF and an external SCD. The keys may be moved in either direction.

KIF Requirements	Ref
B.4.1 Keys shall not be installed in any KLD/KTD until it has been inspected by qualified staff and a reasonable degree of assurance has been reached that the SCD is an authentic device and has not been subject to any unauthorised physical or logical modifications or substitution. This assurance may take the form of, but not limited to, one or more of the following methods using approved guidelines from the supplier on how this is to be done: (a) Physical inspection and/or testing of the equipment immediately prior to key loading; and (b) Physical protection of the equipment. (e.g., bonded carrier, device authentication code injected by Terminal vendor and verified on receipt, tamper evident packaging, etc.).	2

[99] Amended effective 20/8/18, version 007 r&p 001.18

KIF Requirements	Ref
B.4.2 A KLD/KTD shall be an approved SCD designed for the purpose of transporting keys outside the KIF.	47
B.4.3 The KLD/KTD shall not retain a key or, information that may disclose that key, that it has successfully transferred.	47
B.4.4 The KLD will not output any key except when under dual control. Such dual control is enforced by means such as the following: (a) the device requires that at least two passwords be correctly entered within a period of no more than five minutes, before the device will output a key; (b) the device requires that at least two different, non-reproducible physical keys be concurrently inserted into the unit before it will output a key.	49
B.4.5 Controls are in place to ensure the destruction of any old keys from a KLD/KTD returned to the KIF prior to the injection of new keys.	
B.4.6 No person with existing or prior access to any mechanism used to enforce dual control on the KLD/KTD (e.g., password or physical key) has existing, prior, or future access to any other mechanism used to enforce dual control on that device.	23 & 51
B.4.7 If the KLD/KTD only requires tamper evidence then, when the device is not in active use, undetected access to its internal circuitry is prevented by means such as the following: (a) the facility where the KLD/KTD operates has sufficient supervision and controls to detect any such unauthorized access to the KLD/KTD before the device is subsequently put into active use; (b) the KLD/KTD is stored under dual control, in a tamper-evident cabinet for which each incident of opening and closing is controlled and recorded, under dual control; (c) the tamper-evident cabinet, if used, is regularly monitored by at least two trusted people who are qualified to detect and able to observe any unauthorised access.	52

KIF Requirements	Ref
B.4.8 If the KLD/KTD only requires tamper evidence then, when the KLD is in or ready for active use, undetected access to its internal circuitry is prevented by means such as the following: (a) the facility where the KLD/KTD operates has sufficient supervision and controls to detect any such unauthorized access to the KLD/KTD before the KLD/KTD is subsequently used for any cryptographic function; (b) the KLD/KTD is under the continuous supervision of at least two trusted people who are qualified to detect and able to observe any such access.	53
B.4.9 The KLD/KTD is loaded with a plaintext key only under the direct supervision of at least two authorized people, both of whom ensure that there is no “bug” or other disclosing mechanism in the path that the key traverses from the key generation device to the KLD/KTD.	58
B.4.10 The KLD is used to inject a plaintext key into a cryptographic device only under the direct supervision of at least two authorized people, both of whom ensure that there is no “bug” or other disclosing mechanism on the path that the key traverses from the KLD to the target device.	50
B.4.11 Use of any KLD/KTD shall be monitored and a log of all key-loading activities maintained for audit purposes.	59

B.5 General Key Management

KIF Requirements	Ref
B.5.1 Keys shall exist only in those forms permitted by these requirements.	6
B.5.2 Documented procedures exist and are followed to ensure secret or private keys shall be generated using a process such that it is not possible to predict any secret value or to determine that certain values are more probable than others from the total set of all the possible values.	10

KIF Requirements	Ref
B.5.3 A person with access to one component of a key, or to the media conveying this component, shall not have access to any other component of this key or to any other medium conveying any other component of this key.	9 & 63
B.5.4 Functionality needed to import, export, or transfer cryptographic keys from external sources ensures that the keys are in one or more of the following forms: (a) enciphered under the proper variant of a symmetric key encipherment key; (b) enciphered under the asymmetric public key of the recipient; (c) enciphered with an import key being specifically enabled for a limited time and limited number of function calls; (d) as key components managed under dual control, such that two operators are required to perform any key operation; (e) input under dual or multiple control through the secure operator interface, in components such that full knowledge of all but one component gives no usable information on any bit of the cryptographic key; (f) public keys are entered under dual control or enciphered under the a KLD or a target device as per these requirements; (g) Output as clear text keys under dual or multiple control for injection into a KLD or a target device as per these requirements; (h) Output as clear text keys under dual or multiple control for injection into a KLD or a target device as per these requirements.	15 & 62
B.5.5 The transfer of a key to another SCD: (a) uses a secure communications path; or (b) uses a key transfer device; or (c) uses a secure cryptographic path; or (d) is carried out in a secure environment.	4

KIF Requirements		Ref
B.5.6	Storage of the private key requires that secrecy and integrity are ensured. Storage of the public key requires that authenticity and integrity are ensured.	77
B.5.7	Plaintext private and secret key(s) whose compromise would affect only one party shall exist only within a SCD or a physically secure environment operated by, or on behalf of, that party under dual control and split knowledge.	60
B.5.8	Plaintext private and secret key(s) whose compromise would affect multiple parties shall exist only within a SCD.	61
B.5.9	Transport of public keys shall be conveyed in a manner that protects their integrity and authenticity and provides the ability to validate that the correct key was received. The mechanism used to validate that the correct public key was received shall be independent of the actual conveyance method.	62
B.5.10	Key confirmation is often provided by subsequent use of an established key, and if something is wrong with its use then it is immediately detected. This is called implicit key confirmation. Explicit key confirmation in this case may be unnecessary.	80

KIF Requirements	Ref
B.5.11 One or more of the following techniques shall be used to ensure public key integrity: (a) sign the public key and associated data using a digital signature system, thereby creating a public key certificate. Key certificates, and the management of the keys used to create and verify the certificates, are described in Reference 10, Clauses 5.3 and 6 (see KIF Audit Guide); (b) create a MAC for the public key and associated data, using an algorithm defined by ISO 16609 and a key used only for this purpose; (c) store the public key in an SCD; (d) distribute the public key over an unprotected channel, and distribute a key verification code of the public key and associated data over an integrity assured channel such as an authenticated channel with dual controls (key verification is described in Reference 10, Clause 5.5 - see KIF Audit Guide); (e) using authenticated encryption; (f) when entering the public key into an SCD it shall be managed under dual control.	78
B.5.12 The devices (SCDs) involved in using public key schemes shall check the validity of other such devices involved in the communication prior to any key transport, exchange or establishment. Validation of authentication credentials shall occur immediately prior to any key establishment.	87
B.5.13 Any single clear text key component is, at all times during its transmission, conveyance, or movement between any two organizational entities: (a) under the continuous supervision of a person with authorized access to this component; or (b) locked in a security container (including tamper evident packaging) in such a way that it can be obtained only by a person with authorized access to it; or (c) in a physically secure SCD.	64

KIF Requirements		Ref
B.5.14	When plaintext public keys are stored and are not in the form of a certificate or when their certificate has been checked and they will be used without re-checking the certificate, integrity and authenticity shall be ensured. Protection against substitution of the public key during storage is essential. For example, the substitution of a public key used for encipherment may result in a threat to data secrecy. One means of protecting a public key against substitution is to implement the same techniques as for a private key. Another means is to store the public key in a certificate, allowing verification of the key's integrity and authenticity before use. The unauthorized substitution of stored public keys shall be prevented by one or more of the following means: (a) physically and procedurally preventing unauthorized access to the key storage area; (b) storing a key enciphered as a function of its intended use and ensuring that it is not possible to know both a plain text value and its corresponding cipher text, enciphered under the key encipherment key; (c) storing a certificate containing a public key and verifying the certificate prior to its use; the authenticity and integrity of the public key used to verify the certificate shall be ensured. If unauthorized key substitution is known or suspected, procedures are in place and followed to ensure that the public key is replaced with the correct public key.	79
B.5.15	The components of encryption keys shall be transferred using different communication channels per component, such as different courier services to ensure split knowledge.	65
B.5.16	Mechanisms shall exist to ensure that only authorized custodians have access to plaintext key components and place key components into tamper-evident packaging for transmittal and that only authorized custodians open tamper-evident packaging containing key components upon receipt.	66
B.5.17	Unencrypted keys are entered into host HSMs and PEDs using the principles of dual control and split knowledge.	68

KIF Requirements		Ref
B.5.18	The mechanisms used to load keys, such as Terminals, external PIN pads, key guns, or similar devices and methods are protected to prevent any type of monitoring (e.g., visual or logical) that could result in the unauthorized disclosure of any component.	69
B.5.19	Cryptographic keys are only used for their sole intended purpose and are never shared between production and test systems.	73
B.5.20	The following requirements are the minimum standards to be applied to Key Encrypting Keys: (a) All Key Encrypting Keys used to transmit or convey or otherwise secure other cryptographic keys are (at least) as strong as any key they are securing; (b) A double-length DEA 3 key shall be enciphered by a DEA 3 key, an RSA key with a key modulus of at least 1024 bits, or an AES key of at least 128 bits. RSA keys encrypting keys greater in strength than double length DEA 3 keys shall use a modulus of at least 2048 bits. An RSA key with a modulus of at least 1536 bits should be used to encipher double length DEA 3 keys where ever possible;[100] (c) A triple-length DEA 3 key shall be enciphered by a triple-length DEA 3 key, a 128 bit AES key, or an RSA key with a modulus of at least 2048 bits.[101]	67
B.5.21	The use of RSA keys with a modulus of only 1024 bits shall be treated as single use keys; DEA 3 key transport keys shall be treated as single use keys and destroyed after use.[102]	67
B.5.22	Procedures exist to prevent or detect the unauthorized substitution (key replacement and key misuse) of one key for another or the operation of any cryptographic device without legitimate keys.	72

[100] Amended effective 17/10/25, version 017 r&p 001.25
[101] Amended effective 17/10/25, version 017 r&p 001.25
[102] Amended effective 17/10/25, version 017 r&p 001.25

KIF Requirements		Ref
B.5.23	Any known or suspected compromised key and its subsidiary keys (those keys enciphered with the compromised key) shall be replaced with a value not feasibly related to the original key.	75
B.5.24	Key variants are only used in devices that possess the original key. Key variants are not used at different levels of the key hierarchy e.g., a variant of a key encipherment key used for key exchange cannot be used as a working key or as a master file key for local storage.	76
B.5.25	Secret and private keys and key components that are no longer used or have been replaced are securely destroyed.	81
B.5.26	Access to secret and private cryptographic keys and key material shall be limited to a need-to-know basis so that the fewest number of key custodians are necessary to enable their effective use.	82
B.5.27	Each person acting as a key custodian shall be designated as such and this designation documented on a Key Custodian Form which designates each custodian's responsibilities and duties. Each custodian shall sign the Key Custodian Form as having read and understood these responsibilities and duties in relation to the key material entrusted to them.	82
B.5.28	Logs are kept for any time that keys, key components, or related materials are removed from storage or loaded to a SCD.	83
B.5.29	Backups of secret and private keys shall exist only for the purpose of reinstating keys that are accidentally destroyed or are otherwise inaccessible. The backups shall exist only in one of the allowed storage forms for that key.	84
B.5.30	Documented procedures exist and are demonstrably in use for all key management operations.	85

Next page is Annexure C

Annexure C. DEBIT CARD FRAUD PREVENTION - GUIDELINES

[Informative]

Annexure C is Confidential

Next page is Annexure D

Annexure D. COMPROMISED DEVICE MANAGEMENT FRAMEWORK

[Informative]

Annexure D is Confidential

The next page is Annexure E

Annexure E. SECURITY CHECKLISTS FOR INSTALLATION OF EFTPOS TERMINALS[108]

[Informative]

Annexure E is Confidential

Next page is Annexure F

Annexure F. ISSUER AND ACQUIRER BEST PRACTICE GUIDELINES FOR CARD NOT PRESENT TRANSACTIONS[117]

[Deleted]

END

[117] Deleted effective 1/1/20, version 010 r&p 002.19